2011-03

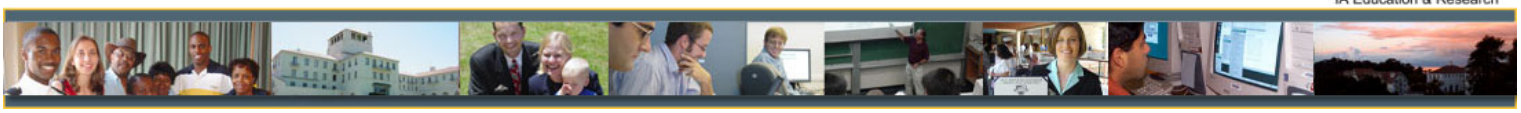
Center for Information Systems Studies Security and Research (CISR) Research: Projects

Naval Postgraduate School (U.S.)

NAVAL POSTGRADUATE SCHOOL
CENTER FOR INFORMATION SYSTEMS SECURITY STUDIES AND RESEARCH

Search Site

Centers of Academic Excellence
IA Education & Research



Research: Projects

The overarching objective of Information Assurance (IA) studies is to improve security in real systems. The CISR program enables students to understand the kinds of technologies that are available to solve current computer security problems and to consider potential future technologies. To this end, our research focuses on using a variety of trusted systems to explore topics in security policy enforcement, security technology for database systems, monolithic and networked trusted computing techniques, and ultimately to develop the training and tools to support trusted systems.

The CISR research program provides a unifying conceptual framework and management structure for long range planning and coordination of focused Information Assurance research projects. The primary program goal is to support the strengthening of assurance provided by the National Information Infrastructure. Our approach includes the research and development of high assurance networks, systems, components and tools, and the open dissemination of outputs from those efforts, such as code and documentation. Open distribution of program outputs provides widespread availability of Information Assurance solutions, as well as clear examples and guidance for high assurance solutions developed elsewhere.

Listed below are CISR's research projects designed to meet these goals.

3Dsec: Trustworthy System Security through 3-D Integrated Hardware
This research will explore the use of 3D integration to enhance system security. 3D integration is a novel way to augment commodity hardware after fabrication, in which a separate silicon layer is bonded onto an existing integrated circuit. Our approach is to use the additional layer to house select security features. This integration decouples the function and economics of security policy enforcement from the underlying computing hardware. As a result, security enhancements are manufacturing options applicable only to those systems that require them, enabling a given design to support, e.g., both a mass-market, and a security-enhanced version. In this research we will identify, design, prototype and test various 3D circuit-level security capabilities, which we expect to significantly assist in reducing both the software complexity often associated with security mechanisms and system vulnerabilities.

CyberCIEGE - Network Security Training Tool
CyberCIEGE is a commercial-grade PC-based 3D video game where players construct a networked computing system and defend it against a variety of attacks.

MYSEA - Monterey Security Architecture
The purpose of this research project is to develop high assurance security services and integrated operating system mechanisms that will protect distributed multi-domain computing environments from malicious code and other attacks.

RCSC - Required Components for Secure Computing
The purpose of the Required Components for Secure Computing (RCSC) project is to investigate the minimal set of specialized components(e.g., those that must be evaluated to meet high assurance requirements) necessary to construct a secure system.

RCsec
The goal of the Reconfigurable Security project is to devise a run-time management system that will provide for the provable adaptable compartmentalization within reconfigurable devices such as FPGAs. This research, which NPS is conducting in conjunction with UCSB, will result in a foundation from which future security work in reconfigurable devices can proceed.

SecureCore
The SecureCore project will investigate the fundamental architectural features required for trustworthy operation of mobile computing devices such as smart cards, embedded controllers and hand-held computers.

TCX - Trusted Computing Exemplar Project
The purpose of the Trusted Computing Exemplar project is to provide a working example to show how trusted computing systems and components can be constructed.

Past Projects

Avionic Authentication Project
This project will design and develop a prototype for continuous authentication of aircraft personnel in order to determine whether the persons flying a given aircraft are authorized to do so.

Emergency Response for Cyber Infrastructure Management
The objective of this research is to investigate architectural mechanisms to provide an emergency response capability for Cyber Infrastructure management through the use of distributed, highly secure, protected domains.

High Assurance MLS LAN - Multi-Level Secure Local Area Network
This project examines a cost effective, multi-level, easy to use office environment leveraging existing high assurance technology.

ISAKMPD
Works in tandem with IPsec to provide secure peer-to-peer connectivity between two systems over a network. The isakmpd_mon provides an isakmpd GUI monitor

for observing aspects of this connectivity

MSHN - The Management System for Heterogeneous Networks
This research is part of the DARPA/ITO Quorum program which is developing technologies that allow end users to achieve predictable and controllable end-to-end quality of service (QoS) for critical defense computing needs in a global heterogeneously distributed computing environment.

PKI - Public Key Infrastructure
CISR has begun research work toward producing a web-based PKI end-user training tool that will provide prospective PKI users with a working knowledge of the infrastructure's underlying functionality. Successful completion of this training could be used as a precursor to CAC (DoD smart card) issuance to DoD employees.

QoSS - Quality of Security Service
This body of work provides theoretical foundations and worked examples for dynamic security policies and services. The resulting conceptual framework encompasses Quality of Protection, Adaptive Security, Dynamic Security, Policy-Based Access Control, and Risk Adaptable Access Control (RADAC).

Security Domain Model
The purpose of this project is to present a formal domain-specific model for security, as a means of conducting automated static analysis of programs for adherence to a security policy. In doing this, we present a precise, formal definition for information flows and covert channels, based on control flow dependency tracing through program execution.

SIPL - Secure Internet Programming Languages
Our research aims to incrementally develop a secure-flow logic for a deterministic, imperative programming language. Simply put, SIPL is a holistic environment for developing secure software.

SKPP - Separation Kernel Protection Profile
The purpose of the Separation Kernel Protection Profile (SKPP) project is to research, design, create, and support the review and validation of a Common Criteria protection profile for high assurance separation kernels. The result of this project is the *U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness*, which was produced in partnership with the Mitre Corporation, under the sponsorship of the NSA. **UDP and Collaboration Services**

Collaboration tools are becoming embedded in the business processes of many enterprises. These tools may include many different communication functions such as e-mail, distributed file-sharing systems, Internet Relay Chat, shared "white boards," video, voice, etc.

VMM - Virtual Machine Monitors
This research addresses the problem of implementing secure Virtual Machine Monitors (VMM) on the Intel Pentium architecture. A VMM allows multiple operating systems to run concurrently under virtual machines on a single workstation.

This page was last modified: March 2011